

Abstract of the Disclosure

The invention provides for hardware processing of ACLs and thus hardware enforcement of access control. A sequence of access control specifiers from an ACL are recorded in a CAM, and information from the packet header is used to attempt to match selected source and destination IP addresses or subnets, ports, and protocols, against all the ACL specifiers at once. Successful matches are input to a priority selector, which selects the match with the highest priority (that is, the match that is first in the sequence of access control specifiers). The specified result of the selected match is used to permit or deny access for the packet without need for software processing, preferably at a rate comparable to wirespeed. The CAM includes an ordered sequence of entries, each of which has an array of ternary elements for matching "0", "1", or any value, and each of which generates a match signal. The ACL entered for recording in the CAM can be optimized to reduce the number of separate entries in the CAM, such as by combining entries which are each special cases of a more general access control specifier. A router including the CAM can also include preprocessing circuits for certain range comparisons which have been found both to be particularly common and to be otherwise inefficiently represented by the ternary nature of the CAM, such as comparisons of the port number against known special cases such as "greater than 1023" or "within the range 6000 to 6500".